SHA-256 Overview

18 March 2011

Debbie Mitchell
DoD PKI PMO
dmmitc3@missi.ncsc.mil

What is SHA-256?

- Many algorithms and schemes that provide a security service ***use a hash*** function as a component
- **Secure Hash Algorithm (SHA)** is an example of a one-way secure hash function
- Works by taking an input of **arbitrary** length and outputs a **fixed** length bit string
  - (One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and
  - (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output
- Cryptographic Hashes approved for use by the USG: *SHA-1*, SHA-224, SHA-256, SHA-384 and SHA-512
- SHA-256 is being used in Federal PKI
  - Commercial availability
  - In line with movement to Suite B Cryptography

Why SHA-256

- Risks of continued use of SHA-1 based on Moore's Law
- 80-bit security strength for cryptography does not provide an acceptable level of protection
- Theoretical attacks on SHA-1 algorithm
- A minimum of eighty bits of security was acceptable until 2010
- Starting in 2011 until 2030, a minimum of 112 bits of security strength is strongly recommended

SHA-1 provides < 80 bits of security when used with digital signatures

Policy Drivers for SHA256

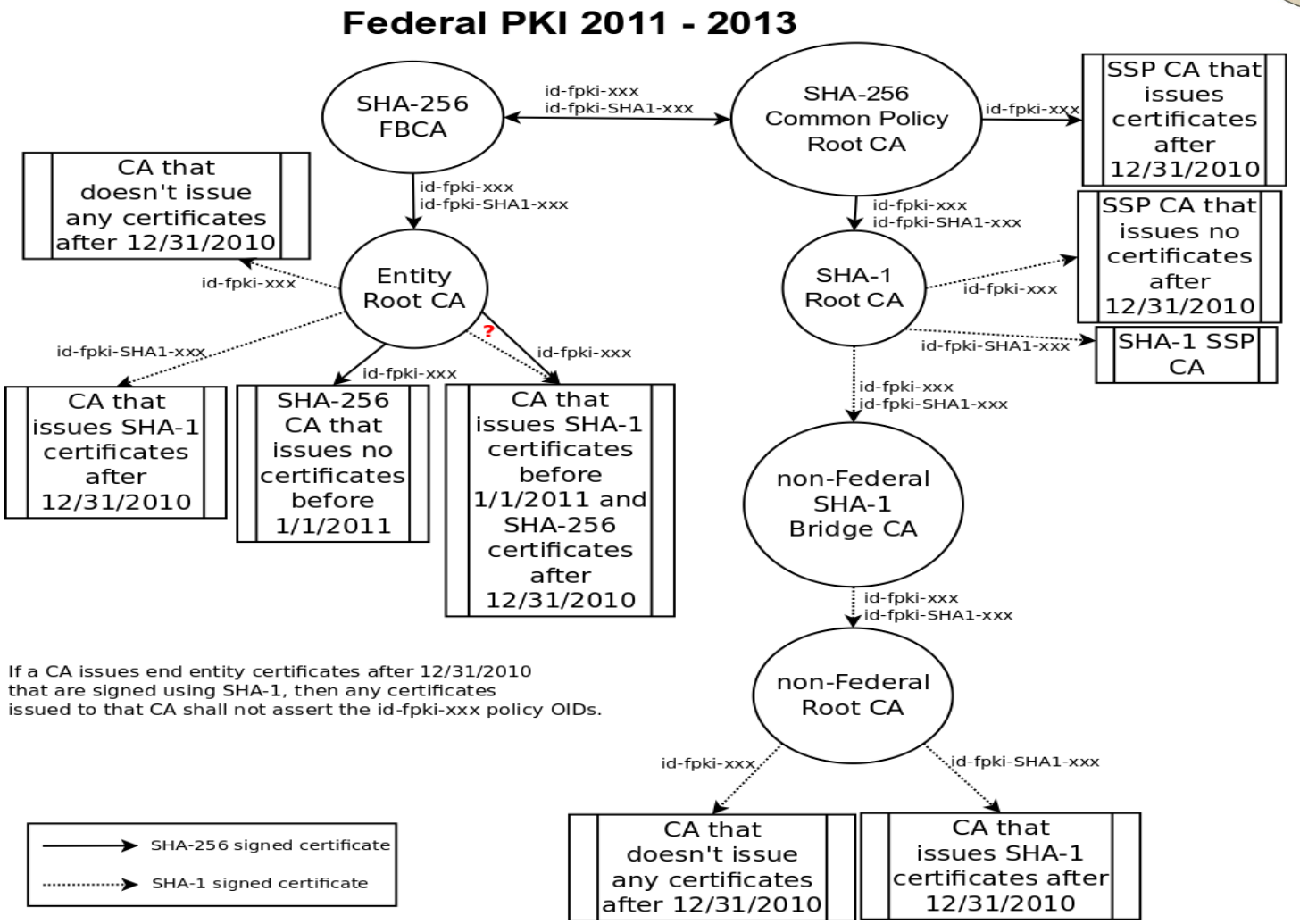
Policy/ Guidance	
NIST SP 800-57, *Recommendation for Key Management – Part 1*	Requires the use of SHA-256 in all digital signatures generated, beginning on January 1, 2011
NIST SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV)*	Requires the use of SHA-256 in all digital signatures generated by CAs signing PIV Cards, beginning on January 1, 2011
NIST SP 800-131A , *Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Sizes*	Deprecated use of SHA-1 until 31 Dec 2013 in some cases. After 31 Dec 2013, key lengths providing less than 112 bits of security strength **shall not** be used to **generate digital signatures**
Federal Bridge and Common Policy Framework Certificate Policies	Requires SHA-256 for PIV and PIV-I certs, objects, CRLs starting 1 JAN 2011 **Deprecated** use of SHA-1 until 31 Dec 2013 after which not allowed
OMB M -11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12*	Mandates the use of PIV credentials for access to federal facilities and information systems

Growing Need for SHA-256

- Beyond Security, Compliancy and Interoperability will feed **utilization**

HSPD 12	Presidential Directive - Secure and reliable identification for **ALL** Federal Executive Branch Agencies (*SHA256 required beginning 01/01/2011*)
FIPS 201 & SP's	Standard Developed in response to HSPD-12. **ALL** Federal Executive Branch Agencies Need to comply with Standard and Supporting pubs to meet HSPD-12 (*SHA256 required beginning 01/01/2011*)
FBCA & Common Policy Framework CP's	Certificate Policies Incorporate recommendations for algorithms and key sizes, and strengths. Federal Agency PKIs need to meet requirements to be **PIV** issuers. Non Federal Agencies need to meet requirements to be **PIV-I** issuers (*SHA256 required for PIV and PIV-I beginning 01/01/2011*)
OMB M11-11	Requires **ALL** Federal Executive Branch Agencies to use PKI and PIVs for authentication to both physical and logical Federal resources (*SHA256 required for PIV beginning 01/01/2011*)

FEDERAL PKI ARCHITECTURE



UNCLASSIFIED